REMARKS

Favorable reconsideration of this application in view of the above amendments and the following remarks is respectfully requested. By this Amendment, claim 4 has been amended, and new claims 41-44 have been added to more fully claim the subject matter of the instant application. Applicant submits that no new matter has been added, and notice to that effect is respectfully requested. Currently, claims 1-44 are pending of which claims 1 and 19 are independent.

The Examiner is thanked for the indication of allowability of claims 9, 10, 15, 18, 26-28, 31, 32, 37, and 40, if rewritten in independent form including all of the limitations of the base claim and intervening claims.

Claim 3 stands rejected under 35 USC 112, first paragraph, as failing to comply with the enablement requirement. This rejection is respectfully traversed. The Examiner does not believe that the specification sufficiently describes to one of ordinary skill in the art how exclusive-ORing (XORing) bits making up input elements with random data can provide output elements that are a random permutation of the input elements. Applicant respectfully directs the Examiner, for instance, to page 12, lines 12-18, and page 17, lines 7-13, of the specification, which describe the use of the term "random" and the use of "random" bits. In particular,

> As used herein, the term "random" refers to a sequence, process or data having random-like properties. In most practical applications, the random process or sequence of data must be deterministic in that the same set of inputs or conditions will repeatedly produce the same "random" result every time. Thus, when randomly encoding transmission signals in a deterministic manner, the encoding is predictable to an intended recipient capable of reproducing the random encoding, but is unpredictable to unintended third parties, making it difficult or impractical for the third party to anticipate or decipher the random encoding.

As further described, for instance at page 17, lines 7-13,

> the invention ... produces permutations of a certain kind that happens to have these properties [random permutations with

> uniform probabilities for all possible movements of each position]. More precisely, each implementation of the invention produces a permutation that is controlled by a set of "random" bits. If these "random" bits are perfectly random, that is, are unbiased and independent choices, then the permutations will be uniform in the manner described.

Further, as described in the specification beginning at page 13, lines 17-20, and referring to FIG. 2, an exclusive-OR operation is performed between time count bit T0 and random bit R0 to obtain the output hop code bit H0. In a repeating loop, the hop code bits are determined. The hop code bits are clocked into a register until all output data elements have been generated from the data elements in the input block. The output elements form an output block of data elements, but in a permuted order using the same random data in processing the entire block of data elements, a permutation of the input elements is generated.

As Applicant has carefully explained the meaning of the word "random" in the specification and explained the use of the random data in an exclusive-OR operation to generate output data elements, Applicant submits that claim 3 is sufficiently described in the specification to meet the enablement requirement. Accordingly, withdrawal of this rejection is respectfully requested.

Claim 4 stands rejected under 35 USC 112, second paragraph, for alleged indefiniteness. This rejection is respectfully traversed. The Examiner does not understand how the random symbol can be retrieved using an address comprising symbols of the output data element when the data element is determined as a function of the random symbol.

Applicant respectfully directs the Examiner to the specification at page 12, line 32 through page 15, line 11, which describes in great detail how the random symbol can be retrieved using an address comprising symbols of the input data element and the output data element. A key point to understand is that, while a multi-symbol output data element can be formed in a single clock pulse, the output data element is nevertheless formed via a "ripple delay" process, wherein individual symbols of the multi-symbol output data element are formed in sequence

during the clock pulse, such that certain symbols of the multi-symbol output data element are formed prior to others and can therefore be included in the address used to form subsequent symbols of the multi-symbol output data element (again, this can all occur during a single clock pulse). Note that this is clarified directly in Fig. 2, which includes a bracket around the relevant portion of the flow chart with the text "occurs within hop clock pulse width." Thus, symbols from the output data element can indeed be used in an address used to retrieve a random symbol. Claim 4 has been reworded slightly to clarify that the claim language further limits the method of claim 1; thus, patentable weight should be accorded to the claim language of claim 4. Accordingly, the Examiner is respectfully requested to reconsider and withdraw the rejection of claim 4.

Claims 1, 2, and 11 stand rejected under 35 USC 102(b) as anticipated by Ritter, "Transposition Cipher with Pseudo-Random Shuffling: The Dynamic Transposition Combiner" (hereinafter, "Ritter"). Claims 3, 14, and 16 stand rejected under 35 USC 103(a) as unpatentable over Ritter. Claims 12 and 13 stand rejected under 35 USC 103(a) as unpatentable over Ritter in view of Dent, U.S. Patent No. 4,476,566 (hereinafter, "Dent"). Claim 17 stands rejected under 35 USC 103(a) as unpatentable over Ritter in view of Mansoorian et al., U.S. Patent No. 6,400,824 (hereinafter, "Mansoorian"). Claims 4, 19, 20, 22-25, 33, 36, and 38 stand rejected under 35 USC 103(a) as unpatentable over Ritter in view of Devereux et al., U.S. Patent No. 4,876,659 (hereinafter, "Devereux"). Claims 7, 8, 21, 29, 20, 34, and 35 stand rejected under 35 USC 103(a) as unpatentable over Ritter and Devereux in view of Dent. Finally, claim 39 stands rejected under 35 USC 103(a) as unpatentable over Ritter and Devereux in view of Mansoorian. Applicant respectfully traverse these rejections for the following reasons.

Claim 1 sets forth a method of generating a random permutation of a block of data elements. The method includes: 1) generating an input block of data elements, wherein each data element occupies a particular position in the input block and each data element is represented by plural symbols; and 2) for each data element in the input block, conditionally changing the value of individual symbols of the data element in accordance with random data to

form an output data element in a corresponding position in an output block of data elements, the output data element being one of the data elements in the input block, wherein each data element is mapped from a position in the input block to a position in the output block, such that the output block of data elements is a random permutation of the input block of data elements. Independent apparatus claim 19 includes comparable requirements.

The Examiner focuses on the "Dynamic Transposition Cipher" section of Ritter (and other subsequent related text) as the primary basis for rejecting the independent claims. The cited section of Ritter describes a byte-shuffling permutation scheme in which multi-bit (byte) elements of a block of data are permuted using pseudo-random data (e.g., each element is one of twenty-six possible alphabetic characters, and the block is a block of text). Ritter clearly explains that the "plaintext will be collected into a block, then a controller will walk through the block, byte-by-byte, exchanging each byte with "partner" bytes selected by a random number generator." Ritter contrasts this byte-level permutation with a bit-level permutation scheme at length.

While the subject invention produces a random permutation of a block of multi-symbol data elements, the technique for accomplishing this random permutation is fundamentally different from what is disclosed by Ritter and these difference are clearly reflect in claims 1 and 19. In particular, as recited in claims 1 and 19, the output data element is generated by conditionally changing the value of *individual symbols* of each data element in the input block. In other words, the mechanism by which permutation of multi-symbol data elements is accomplished involves operating on the individual symbols within the data elements. Ritter does not disclose or fairly suggest such a mechanism. In contrast, Ritter describes a controller that walks through the block, byte-by-byte, exchanging each byte with partner bytes. There is no suggestion in Ritter to perform permutation of multi-symbol data elements by operating on the individual symbols within a multi-symbol element, as required by claims 1 and 19. In fact, Ritter clearly distinguishes bit-level permutations from byte-level permutations (see, e.g., page 5

of Ritter) and does not suggest anywhere that byte-level permutations can be accomplished with bit-level mechanisms.

Moreover, the secondary references, cited by the Examiner in connection with subject matter recited in a number of dependent claims, do not make up for the deficiencies of Ritter, since none of these references discloses or suggests conditionally changing the value of individual symbols of a multi-symbol data element in accordance with random data to form an output data element in a corresponding position in an output block of data elements, as required by parent claims 1 and 19. Thus, the subject matter of parent claims 1 and 19 and their dependent claims would not have been (and could not have been) obvious from any combination of Ritter, Dent, Mansoorian, and Devereux. Accordingly, the Examiner is respectfully requested to reconsider and withdraw the rejections of the claims over these references.

New claims 41 (41/1) and 43 (43/19) require that an input block of 2^N data elements data elements be permuted using no more than $N \cdot 2^{N-1}$ random bits. Support for this subject matter is found in Applicant's specification (see, e.g., page 16, lines 21-29). None of the cited references discloses or suggests this subject matter. Note, in particular, that Ritter suggests in the first paragraph on page 9 that substantially more bits are required for a comparable permutation (i.e., a permutation of a 2^N-byte block requires $12*2^N$ pseudo-random bits).

New claims 42 (42/1) and 44 (44/19) require using random data to permute the input block of data elements to the output block of data elements such that not all possible permutations of the input block of data elements are equally probable, but data elements in each position in the input block of data elements have an equal probability of being mapped into any position in the output block of data elements. Support for this subject matter is found in Applicant's specification (see, e.g., page 16, line 29 through page 17, line 6). None of the cited references discloses or suggests this subject matter.

In view of the foregoing, Applicant respectfully submits that all pending claims are in condition for allowance, and formal notice of such is solicited. If the Examiner has any

questions or comments, the Examiner is respectfully requested to contact the undersigned at the number listed below.

Filed concurrently herewith is a Petition (with payment) for an Extension of Time of one month. Also filed herewith is an excess claim fee for four claims in excess of the forty previously paid for. Applicant hereby petition for any extension of time which may be required to maintain the pendency of this case, and any required fee for such extension is to be charged to Deposit Account No. 05-0460.

EDELL, SHAPIRO & FINNAN, LLC
CUSTOMER NO. 27896
1901 Research Boulevard, Suite 400
Rockville, MD 20850
(301) 424-3640

Hand Delivered on: September 7, 2004

Respectfully submitted by
EDELL, SHAPIRO & FINNAN, LLC

By: _____
Patrick J. Finnan
Reg. No. 39,189